Camp CryptoBot: A Method for Taking Risks and Motivating High School Girls to Pursue a Career in Cybersecurity

Pauline Mosley[1], Lisa Ellrodt[2], Doris Ulysse[3]

Pace University, Seidenberg School of Computer Science and Information Technology, United States[1, 2, 3]

Abstract

Why aren't female students majoring in cybersecurity when this is the fastest growing field?[1] How come only 24 percent of the U.S. workforce in cybersecurity is female? [2,6] This gender disparity is concerning, and the challenges women face in the cybersecurity sector are puzzling. These challenges either prevent them from entering or force them to leave. The gender imbalance has potential consequences for this nation's security, so it is imperative that we understand why women are not being attracted to this field. One study suggests that this shortage is because women believe that they will not succeed at STEM courses. They have a "perceived risk of failing". Perceived Risk of Failing refers to high school students' perception that they are incapable of understanding STEM subjects and will fail if they pursue STEM courses. NSF data revealed that in 2010 only 7.5 percent of engineering or computer science technicians were African American or Hispanic. [3]

It is recognized that women have made strides in closing that gap we still have a substantial way to go. [4] According to a recent survey by Women in Tech "28% of C-suite leaders are women and 5% represent racial minority". Camp CryptoBot utilizes SeaPerch (underwater robot) and Sphero (round robotic ball) as the platform for teaching cryptography and cybersecurity concepts using various pedagogical approaches, including storytelling, hands-on labs, and problem-solving missions. In our paper we will share our methodologies for increasing female interest in cybersecurity and which methodologies were effective on reducing their fear of failure thereby increasing their self-efficacy.

Keywords: *cybersecurity, gender gap, retention, sphero, SeaPerch, STEM*

1. Introduction

This paper describes an effort at Pace University (PU) to increase the participation of women in Cybersecurity. Pace University has been a National Center of Academic Excellence in Cybersecurity Education since 2001, and has been giving scholarships under the SFS program since 2002. PU has awarded CyberCorps Scholarship for Service (SFS) scholarships to 148 students since 2001. Which is an average of 6-7 students per year. Increasing the number of women participating in cybersecurity activities may provide incentive for more women to apply for these disciplines as well. Based on participation in the first five years of operating Camp CryptoBot, and on exit surveys conducted at the end of the camp, it appears as if a significant percentage of the women participating in the summer camp are inclined to apply for a computing discipline. Since they are rising juniors and seniors, our research does not follow them through college so further research needs to be done to see if their interest is sustainable.

2. Camp Cryptobot Methodology

Camp CryptoBot, consists of three core modules (CAST, CDSL and CryptoBot Missions) which demonstrate and teach the ten principles with an emphasis on cryptography. This curriculum is ultimately intended to enable full inter-modular "team teaching". Every day we introduce two first principles using a skit. These two principles are discussed during the cooperative activity and implemented during the CryptoBot mission. The umbrella structure of the curriculum highlights the fact that programming, problem-solving, cryptography concepts, and cybersecurity cannot be taught in a vacuum. The more students are able to see and study cryptography and the challenges of keeping data secure, the more authentic and nuanced their inquiry becomes. This point cannot be overstated. While not all students will be inclined to pursue cybersecurity as a result of this camp, the goal is to instill essential cybersecurity first principles and concepts in all students such that they may carry over into any field-academic, artistic, economic, or otherwise-they may pursue. The culminating events simulated warfare challenge and treasure hunt requires students to infuse learning from all modules and all first principles. The camp schedule is listed below.

8:30AM-9:00AM	Breakfast
9:00AM-9:15AM	Daily First Principles and Learning Outcomes
9:15AM-10:30AM	Cryptography Applied Skills Training - CAST
10:30AM-11:00AM	Morning Break
11:00AM-12:00PM	Cooperative Learning Action Game - CLAG
12:00PM-1:00PM	Lunch
1:00PM-2:30PM	CryptoBot Missions (Hands-on lab)
2:30PM-2:45PM	Daily Squawk (Student Reflective Survey)
2:45PM-3:00PM	Afternoon Break
3:00PM-4:00PM	Class Discussion, Reflection, and Mission Status Reports

3. Cryptobot Curriculum

Table 1 below shows the prospectus of the camp on a daily basis. Each of these components require students to take risks as well as cultivate their interest which effectively increases student motivation. The daily lessons will be comprised of three components: Cryptography Applied Skills Training (CAST), Cooperative Drone or SeaPerch Learning (CDSL), and CryptoBot Missions. Cryptography will be taught utilizing the ten cybersecurity First Principles and discussed from four perspectives: literacy, science, society, and warfare. The day will begin by introducing two First Principles using skits and hand signals to engage the students. The learning objectives for the day will also be stated in the morning as well as written on the whiteboard. Cryptography topics will be introduced using hands-on laboratory exercises, team activities and individual reflection. Throughout the workshop, high school students will act as Navy Cryptologists, and be engaged in a narrative that interweaves all missions and requires them to apply specific cybersecurity principles using robotic technology. Students are given the rank of Cryptologic Technician Interpretive (CTI), and as they successfully complete each CryptoBot mission they will move up the ranks to Cryptologic Technician Technical (CTT) and then Cryptologic Technician Collection (CTC) until they reach Cryptologic Technician Network (CTN). Each rank will be assigned with different levels of domain access, job description, name badge and resources.

Table 1: CryptoBot Curriculum

Date	**Topics**	**Daily First Principles**	**Rank**
07/23 Mon.	**CRYPTO-LITERACY** Cryptography Applied Skills Training (CAST) • What is My Name? (substitution cipher) • Who is on My Team? (transposition cipher) • Camp Background Story: Cryptologists Induction Ceremony - Navy Cryptography Mission presented by Navy Chief Petty Officer & SeaPerch Overview Cooperative Drone/SeaPerch Learning (CDSL) • Using Drones to find **hidden data** anywhere • Using SeaPerch to find **hidden data** in water • **Layers of security** for Drones and SeaPerch • **Cooperative Activity**: Hide Go Seek CryptoBot Mission #1: (Hands-on Lab) • Design and Construction of SeaPerch CryptoBot • *Mission Status Report (student presentations)*	Data Hiding Layering	CTI
07/24 Tue.	**CRYPTO-TECHNOLOGY** Cryptography Applied Skills Training (CAST) • Team Tasks – Modularity (Caesar cipher) • Team Tasks Domain Access (vigenere table cipher) • Fishbowl Discussion on Information Hiding Cooperative Drone/SeaPerch Learning (CDSL) • Drone Programming – Autonomous Aerial Robotics • SeaPerch and Sensors – Autonomous Detection	Domain Separation Modularity	CTT

	• **Cooperative Activity**: Hack Attack CryptoBot Mission #2: (Hands-on Lab) • Information Hiding Application to Drone and SeaPerch • *Mission Status Report*		
07/25 Wed.	**CRYPTO-SOCIETY** Cryptography Applied Skills Training (CAST) • What is Steganography? • Why Are Security Polices Needed? • Steganography Carousel Brainstorming Cooperative Drone/SeaPerch Learning (CDSL) • Steganography application to Drone/SeaPerch • **Cooperative Activity**: Jigsaw Steganography • *Kahoots CAST Reflection* CryptoBot Mission #3: (Hands-on Lab) • Ciphers and Steganography Tools Using Drones and Seaperch to secure communication • *Mission Status Report*	Abstraction Simplicity	CTN
07/26 Thur.	**CRYPTO-WARFARE** Cryptography Applied Skills Training (CAST) • Correct and Safe Online Behavior Debate • Review all Ciphers (Caesar, Vigenere Table, Transposition, and Pig Pen) Cooperative Drone/SeaPerch Learning (CDSL) • **Cooperative Activity**: First Principles Treasure Hunt CryptoBot Mission #4: (Hands-on Lab) • Simulated Warfare Challenge • *Mission Status Report*	Process Isolation Encapsulation	CTR
07/27 Fri.	**CRYPTO-MISSON REPORTS & PRESENTATIONS** Cooperative Drone/SeaPerch Learning (CDSL) • **Cooperative Activity**: Cryptography Jeopardy • *Final Round Table Mission Kahoots Reflections* • *Final Mission Status Reports* Closing Ceremonies • CryptoBot in Motion & Group Presentations • Keynote Speaker – CISCO • CryptoBot Arcade & Awards and Certificates	Minimization Least Privilege	

3.1 Cryptography Applied Skills Training (CAST)

These sessions focus on the fundamentals of basic cryptography. Students learn various ciphers (Caesar, Vigenere Table, Transposition and Pig-Pen) and apply these ciphers to uncover key information in order to complete the mission. Training is a dynamic 30 minute lecture followed by a 60 minute interactive hands-on cryptography activity that promotes critical thinking and questioning. It also encourages students to take risks and try various thinking strategies. Every morning all participants will be randomly placed into two-person teams, overseen by one student assistant per three two-person teams, that will work together to complete these exercises below:

Table 2: Cryptography Activities

What is My Name?	This ice-breaker game is highly useful for building up team chemistry. Campers will be given their name encrypted. They will have to apply the transposition cipher to decode their own name as well as their peers.
Who is on My Team?	Campers will have to identify other campers that have the same transposition pattern as theirs to determine who is on that team. This is fun and engaging ice-breaker game for the first day of camp.
Camp Background Story	The US Navy personnel will enlist all campers as Navy Cryptologists and state that there is classified information missing somewhere on the Pace campus. The Navy needs their help to retrieve it to help solve the case of Pace's Computer Department being hacked.
Fishbowl Discussion On Information Hiding	Fishbowl is a discussion technique that allows for a richer discussion of any given topic. It frequently builds community among students and demonstrates how different groups collaborate. Students will discuss what properties are inherent in information hiding to achieve a secure system.
Steganography Carousel	In groups students visit stations, each themed with a different steganography

Brainstorming	aspect, for a few minutes. In the first round, students add information to the station. For each subsequent round, students read the information that is already at the station and add new information. After the final station, each group summarizes, by sharing aloud, the information at that station.
Online Behavior Debate	Students will determine the debate topic relating to appropriate online behavior and cyberbullying, research the topic and then debate it.

3.2 Cooperative Drone/SeaPerch Learning (CDSL)

In the CDSL session, students are placed into teams of 11 or 12 students. Based upon the student's skill level or interest 5 or 6 students will be assigned to Drone Learning and 5 or 6 to SeaPerch Learning. Both groups will train separately, but work together as one team during the CryptoBot missions. Student assistants will always be assigned with a sub-team and a teacher will be in the room. Each of interactive gaming-sessions demonstrates the importance and role of the First Principles. The element of fun helps to disguise how they think, ask questions, and explore. Discussions and Kahoots-survey will follow to ascertain if concepts taught in the lecture were comprehended. All of CDSL activities are game oriented which utilized ciphers to illustrate the First Principles. They are listed below in table 3.

Table 3: Drone/SeaPearch Activities

Hide Go Seek	Using the picture, video, and GPS features on the drone and SeaPerch students will be challenged to find 5 pieces of hidden data using both types of robotics.
Hack Attack	Students will think critically as to how to prevent their drone or SeaPerch from being attacked as well as how to communicate securely using cryptic messages.
Jigsaw Steganography	Students working in a group will be given a challenge to collect 5 pictures and extract from these pictures a narrative. Each picture will contain a segment of the narrative. They are to work within their group and arrange the parts in a sequential fashion using Steganography tools. Once all groups have unjumbled their respective parts, all groups work collectively in arranging the parts into one such that the narrative flows correctly.
First Principles Treasure Hunt	This final game requires students to utilized all of the ciphers that they have learned to locate the 10 Principles which are hidden in various places on campus. They will have to put together a series of 3 clues to determine a first principle. They need to find all 10 to complete the hunt. They will be required to use drones and SeaPerches as part of the hunt.
Cryptography Jeopardy	Jeopardy game comprised of cryptography categories and questions with varying degrees of complexity. This game will have the Jeopardy music and requires a computer station with overhead for projection.

3.3 CryptoBot Missions

The CryptoBot Missions (see Table 4) require students to be placed into 4 eleven or twelve member teams. Each CryptoBot Mission is designed for students to demonstrate their understanding of the First Principles by applying cryptography techniques utilizing drones or SeaPerch. There are 4 classrooms designated as labs, which are: Mechanical Lab, Engineering Lab, Drone Lab, and Cryptography Lab. There will be four-three member teams with two student assistants and one teacher in the lab. Hence, there will be twelve students, two student assistants, and one teacher in each lab. The instructor will lecture and the student assistants will work with all student teams making sure that all students are engaged and following the lecture. All components of the lab will be interactive and activity-based so that we will foster teacher-student interaction in a non-threatening but yet highly engaging scaffolding manner. All missions are mapped to the First Principles and this matrix is described below:

Table 4: CryptoBot Missions

#	**First Principles**	**CryptoBot Missions**	**CryptoBot Mission Learning Objectives**
1	Data Hiding Layering	To design and construct 2 SeaPerches with hidden information and a security feature.	• Students will be able to describe why **layering and data hiding** are important to security. • Students will understand the interaction between security and system usability while designing SeaPerch. • Students will be able to think of potential risks or attacks against

			water vehicles like SeaPerch and prepare a method/design to repel attacks.
2	Domain Separation Modularity	To find, retrieve, and decode using various ciphers hidden information in water utilizing SeaPerches.	• Students will understand the importance and advantages to **domain separation and modularity** when problem solving a security breach. • Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation. • Students will be able to describe how crypto can be used, strengths and weaknesses of different ciphers and issues that have to be addressed in an implementation (e.g., key management)
3	Abstraction Simplicity	To find, retrieve, and decode using various ciphers hidden information within pictures utilizing Drones.	• Students will understand the relationships between **abstractions vs. simplicity** and the degree of data confidentiality. • Students will learn how to discover a message hidden using steganography. • Students will create a digital document with a hidden message.
4	Process Isolation Encapsulation	To send a cryptic message securely using SeaPerches and Drones and to have a defense strategy in the advent of a cyber-attack either in air or in water.	• Students will understand the benefits of **encapsulated messages** as well as keeping **processes separate** in order to prevent one process negatively effecting another. • Students will recognize a systems' vulnerability and the possible damage from malfunctions. • Students will recognize the difficulties in managing information resources.
5	Minimization Least Privileged	To reflect on all missions and analyze the strengths and weaknesses encountered during the missions.	• Students will learn the role of minimization and least privileged. • Students will recognize how all 10 First Principles play a role in cybersecurity.

4. Learner-Centered Classroom

The Camp CryptoBot curriculum is a model that utilizes a problem-based cooperative learning approach to subject immersion, idea generation, and hands-on construction. It facilitates a learner-center classroom because pedagogical methodologies can be tailored for various student learning patterns, and multiple strategies can be implemented to engage all students, regardless of gender or race. This type of classroom encourages students, in particularly young women to take risks as well as promote student interest or motivation to learn. Our varied approaches, which are discussion, hands-on activities, debates, etc. encourage students to explore and question how and what they are learning, thereby they begin to define their personal expertise, interests and identity as a learner. These avenues of exploration overlap and merge in organic ways within each student's unique learning experience. Multiple dynamic fun-filled team activities will take place in all of the modules which will reinforce cybersecurity first principles and basic network concepts thereby promoting team dynamics and critical thinking skills. We expect that the participants will learn the following by the end of the camp fundamental concepts in cybersecurity, including basic terminology, attacks and threats, and a basic understanding of cryptography.

5. Conclusions

The problem of a low percentage of women applying for the computer science or cybersecurity programs is really a symptom of a much larger problem. The engineering and computing disciplines have been suffering from low female enrollment for a long time. It is interesting to note, that the majority of students in colleges and universities are women, yet the caveat is the percentage of women in computer science is less than 20% of the total student population. In the book entitled *Unlocking the Clubhouse: Women in Computing*, Allen Fisher and Jane Margolis analyze the reasons why women shy away from the computing curriculums and discovered that one reason is because it is not female-friendly[8]. In another book, *Stuck in the Shallow End: Education, Race and Computing* by Margolis[9], Margolis learned why disadvantaged students in Los Angeles, even when resources are made available to them, do not take advantage of the opportunities as often as other students, because they felt that the computing environment was exclusive and that they did not want to fail. In the famous study conducted by Hill, Corbett, Rose, *Why So Few*? lack of interest and stereotype threat which led to women believing that they would fail at STEM contributed to these women having low self-esteem at STEM courses.

After analyzing the data after five years of operating Camp CrypBot , we believe that our curriculum model promotes student interest as well as minimizes student's risk of failure. According to our exit surveys given at the end of each camp, 70% of the females that have participated in the camp indicated that they are more confident and willing to take risks after participating in Camp CryptoBot. Although our dataset is inclusive and will require further assessments and research, we can conclude that components of our model are making a difference in young women's perception. Several women from varying years have contacted me saying that they now intend to apply to Pace University to study computer science and specialize in cybersecurity. One of the six women participating in the summer research experience has already taken the scholarship and four others have expressed the desire to receive the scholarship. Fifteen students, 8 female and 7 males have chosen Pace University as their home institution and majoring in Information Technology or Computer Science. We are now seeking resources to continue this summer camp and conduct further research studies. In addition, we are offering 1 day cybersecurity workshops for high school students.

There are many summer camp experiences for young woman, however, what sets this camp apart is the consideration factors to enhance female self-efficacy and negate female fear of failing. The design of the lessons is created by women for women to promote inclusion and diversity, as well as to introduce and sustain best practices that encourage women to stay in the field. If you can see it you can become it – another key factor of this model is the diversity of female faculty. In 2020, Camp CryptoBot was held virtually and even in the modality, we were able to create an online environment in which the girls felt supported and were inspired to consider cybersecurity. As a result of this model operating for six years, our findings reveal that the girls participating in this camp showed evidence of growth in self-efficacy through their developing abilities in robotics and programming skills. Our model contributes to the evidence that it is possible to recruit and attract a diverse group of young women to cybersecurity.

6. Acknowledgments

Special thanks to the participants, Unites States Navy Personnel, guest lectures from IBM, Google, and Cybersecurity firms. Thanks to Dark Enterprises for conducting the surveys and assessment for all six camps. This material is based upon work supported by the National Science Foundation, National Security Agency and GenCyber awards: no.#H98230-16-1-0163, #H98230-19-1-0239, #H98230-22-1-0176, #H98230-22-1-0138, and #H98230-21-1-0087.

REFERENCES

[1] Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R., & Segal, A. (2022). *Cybersecurity as an Engine for Growth*. New America..

[2] Toft, R. S. E., & Eikaas, T. C. (2023). The Impact of Gender Equality in the Cybersecurity Sector (Master's thesis, University of Agder).

[3] Henry, M.A., Shorter, S., Charkoudian, L.K. et al. Quantifying fear of failure in STEM: modifying and evaluating the Performance Failure Appraisal Inventory (PFAI) for use with STEM undergraduates. IJ STEM Ed 8, 43 (2021).

[4] "WomenTech Network Survey", https://www.womentech.net/en-us/women-in-tech-stats#7

[5] ISCA Cybersecurity Workforce Study, "Artificial Intelligence are Challenging the Global Cybersecurity Workforce", 2023, ISC2_Cybersecurity_Workforce_Study_2023.pdf.

[6] Security Newswire, "Women Represent 24 Percent of Cybersecurity Workforce, (ISC)2 Reports, April 2, 2019, Women Represent 24 Percent of Cybersecurity Workforce, (ISC)² Reports | 2019-04-02 | Security Magazine

[7] Dampier, D., “Building an Education Program for Engineers in Digital Forensics,” Proceedings of the 2008 ASEE Conference, Pittsburgh, PA, June 22-25, 2008.

[8] Gorski, E., “College 'gender gap' favoring women stops growing”, Seattle Times, January 25, 2010, http://seattletimes.nwsource.com/html/nationworld/2010890292_apuscollegegendergap.html, downloaded January 30, 2010.

[9] Margolis, J. and A. Fisher, Unlocking the Clubhouse: Women in Computing, MIT Press, December 2001.

[10] Margolis, J., Stuck in the Shallow End: Education, Race, and Computing, MIT Press, September 2008.

[11] STEM Jobs See Uneven Progress in Increasing Gender, Racial and Ethnic Diversity https://www.pewresearch.org/science/2021/04/01/stem-jobs-see-uneven-progress-in-increasing-gender-racial-and-ethnic-diversity/